IN THE CLAIMS

Please amend the claims as follows:

1. (currently amended) A computer-readable medium having a computer program product for performing virus detection on a file within ~~whose contents cause~~ a computer system ~~to perform selective virus signature scanning against a target file associated with an executing agent~~, ~~the computer system having an anti-virus program with instructions to perform the steps of~~ said computer-readable medium comprising:

computer program code for categorizing a plurality of ~~organizing~~ virus signatures into a respective one of a plurality of anti-virus sets according to their characteristic, wherein each of said anti-virus sets contains ~~a characteristic shared by all the~~ virus signatures sharing at least one common characteristic ~~within the set~~;

associating an executing agent with a ~~portion~~ subset of ~~the~~ said plurality of anti-virus sets, wherein ~~with the~~ said executing agent is associated with a target file; and

in response to said target file being opened by said associated executing agent, scanning ~~the~~ contents of ~~the~~ said target file for viruses by applying ~~a virus signature which matches a~~ virus signatures stored in ~~the associated one or more~~ said subset of said plurality of said anti-virus sets associated with said executing agent.

2. (currently amended) The computer-readable medium of claim 1, wherein said target file being opened by said associated executing agent is performed by an operating system ~~further comprising a step before the scanning step, the step comprising:~~

~~associating a rule with the executing agent to indicate a manner in which the associated portion of the plurality of anti-virus sets are applied~~.

3. (currently amended) The computer-readable medium of claim 1, wherein said computer-readable medium further includes computer program code for defining a rule to preclude scanning of said target file ~~the associating step includes providing user selectable options~~.

4. (currently amended) The computer-readable medium of claim ~~2~~ 3, wherein said computer-readable medium further includes computer program code for, in response to said rule to preclude scanning of said target file, allowing said target file to execute without scanning said target file for viruses ~~the role applied includes a periodic batch scan of one or more target files~~.

5. (currently amended) The computer-readable medium of claim ~~2~~ 1, wherein said computer-readable medium further includes computer program code for marking said target file has been scanned and allowing said target file to execute in response to a determination that contents of said target file do not match any virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent ~~the manner in Which the associated portion of the plurality of anti-virus sets are applied to executing agent's target files includes a trigger mechanism which invokes subsequent scanning of the executing agent's target files~~.

6. (currently amended) The computer-readable medium of claim ~~5~~ 1, wherein said computer-readable medium further includes computer program code for quarantining said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent ~~the trigger mechanism includes applying the scanning step upon a request for a file operation on the target file~~.

7. (currently amended) The computer-readable medium of claim ~~5~~ 1, wherein said computer-readable medium further includes computer program code for deleting said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent ~~the trigger mechanism includes applying the scanning step periodically on one or more target files associated with the executing agent~~.

8. (currently amended) The computer-readable medium of claim 1, wherein said computer-readable medium further includes computer program code for periodically scanning said target file associated with said executing agent ~~further comprising a step before the organizing step, the step comprising:~~ ~~determining the plurality of executing agents installed on the computer system~~.

9. (currently amended) The computer-readable medium of claim 1, wherein ~~the plurality of anti-virus sets have a first anti-virus set and a second anti-vires set, the organizing step~~ said computer-readable medium further includes ~~comprises~~:

computer program code for arranging ~~the~~ said plurality of anti-virus sets into a hierarchical structure having first and second levels, ~~the~~ wherein said first level ~~having the~~ includes a first anti-virus set containing virus signatures ~~which~~ that are mutually applicable to a plurality of executing agents, ~~the~~ wherein said second level ~~having the~~ includes a second anti-virus set containing virus signatures ~~which~~ that are exclusively applicable to ~~the first portion~~ a subset of ~~the~~ said plurality of executing agents.

10. (currently amended) The computer-readable medium of claim 1 ~~wherein the plurality of anti-virus sets have a first anti-virus set, a second anti-virus set, and a third anti-virus set, wherein the plurality of executing agents has a first portion~~, wherein ~~the organizing step~~ said computer-readable medium further includes ~~comprises~~:

computer program code for arranging ~~the~~ said plurality of anti-virus sets into a hierarchical structure having a first level, a second level, and a third level, wherein ~~the~~ first level ~~having the~~ includes a first anti-virus set containing virus signatures ~~which~~ that are mutually applicable to a plurality of executing agents, wherein said ~~the~~ second level ~~having the~~ includes a second anti-virus set containing virus signatures which are mutually applicable to ~~the first portion~~ a subset of ~~the~~ said plurality of executing agents, wherein said ~~the~~ third level ~~having the~~ includes a third anti-virus set containing virus signatures

~~which~~ that are exclusively applicable to one of ~~the first portion~~ said subset of ~~the~~ said plurality of executing agents.

11-29. canceled.

30. (new) A method for performing virus detection on a file within a computer system, said method comprising:

categorizing a plurality of virus signatures into a respective one of a plurality of anti-virus sets according to their characteristic, wherein each of said anti-virus sets contains virus signatures sharing at least one common characteristic;

associating an executing agent with a subset of said plurality of anti-virus sets, wherein said executing agent is associated with a target file; and

in response to said target file being opened by said associated executing agent, scanning contents of said target file for viruses by applying virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

31. (new) The method of claim 30, wherein said target file being opened by said associated executing agent is performed by an operating system.

32. (new) The method of claim 30, wherein said method further includes defining a rule to preclude scanning of said target file.

33. (new) The method of claim 32, wherein said method further includes computer program code for, in response to said rule to preclude scanning of said target file, allowing said target file to execute without scanning said target file for viruses.

34. (new) The method of claim 30, wherein said method further includes marking said target file has been scanned and allowing said target file to execute in response to a determination that contents of said target file do not match any virus signatures stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

35. (new) The method of claim 30, wherein said method further includes quarantining said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

36. (new) The method of claim 30, wherein said method further includes deleting said target file in response to a determination that some contents of said target file match a virus signature stored in said subset of said plurality of said anti-virus sets associated with said executing agent.

37. (new) The method of claim 30, wherein said computer- method further includes periodically scanning said target file associated with said executing agent.

38. (new) The method of claim 30, wherein said method further includes:

arranging said plurality of anti-virus sets into a hierarchical structure having first and second levels, wherein said first level includes a first anti-virus set containing virus signatures that are mutually applicable to a plurality of executing agents, wherein said second level includes a second anti-virus set containing virus signatures that are exclusively applicable to a subset of said plurality of executing agents.

39. (new) The method of claim 30, wherein said method further includes:

arranging said plurality of anti-virus sets into a hierarchical structure having a first level, a second level, and a third level, wherein first level includes a first anti-virus set containing virus signatures that are mutually applicable to a plurality of executing agents, wherein said second level includes a second anti-virus set containing virus signatures which are mutually applicable to a subset of said plurality of executing agents, wherein said third level includes a third anti-virus set containing virus signatures that are exclusively applicable to one of said subset of said plurality of executing agents.